UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LEAH WALLACE, individually on behalf of herself and all others similarly situated, Plaintiff, v. NUVANCE HEALTH and HEALTH QUEST SYSTEMS, INC. Defendants.	)	**Civil Action No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Leah Wallace ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts respectively pertaining to herself and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against defendant Nuvance Health ("Nuvance") and Health Quest Systems, Inc. ("Health Quest") (all Defendants are collectively referred to as "Defendants").

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for their failure to exercise reasonable care in securing and safeguarding their patients' sensitive personal data—including patients' names, dates of birth, Social Security numbers, driver's license numbers, financial account information, PINs and security codes, payment card information, provider names, dates of treatment, treatment and diagnosis information and health insurance claims information ("Private Information").

2. In July of 2018 Defendants first learned of a "phishing" incident whereby an unauthorized party may have gained access to the emails and attachments of several of Defendants'

employee email accounts that may have contained patients' Private Information (the "Security Breach"). As a result, the Private Information of 28,910 patients was potentially compromised. The initial investigation reaching this conclusion was not completed until April 2, 2019.

3. Despite the investigation concluding in early April 2019, Defendants inexplicably did not begin to notify any potentially affected patients or the public of the breach until late May or early June 2019.

4. On or about January 16, 2020, Defendants announced that, following a second investigation into the 2018 Security Breach, they had discovered that more Patient Data has been compromised during the breach than previously thought, with additional patients having been affected. Defendants stated that they intended to provide direct notice of the Security Breach to patients by February 15, 2020.

5. In a notice mailed to Plaintiff on January 3, 2020, Defendants stated that the second investigation was completed on November 8, 2019, nearly two months before notice was provided to Plaintiff. The notice also recommended that Plaintiff "regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately."

6. Defendants' security failures enabled the hackers to steal the Private Information of Plaintiff and members of the Class (defined below). These failures put Plaintiff's and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Security Breach, including, as appropriate, reviewing records for fraudulent charges and healthcare services billed for but not received,

cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach.

7. The Security Breach was caused and enabled by Defendants' violation of their obligations to abide by best practices and industry standards concerning the security of patients records and payment information. Defendants failed to comply with security standards and allowed their customers' Private Information to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

8. Accordingly, Plaintiff, on behalf of herself and other members of the Class, assert claims for violations of negligence, breach of implied contract, unjust enrichment/quasi-contract, breach of confidence and violation of N.Y. Gen. Bus. Law § 349, and seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

9. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. The Court has personal jurisdiction over Defendants because their principal place of business is located, and they conduct substantial business, in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants maintain their principal place of business in this District and therefore reside in this District

pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

III. PARTIES

Plaintiff

12. Plaintiff Leah Wallace is a resident of Duchess County, New York. Plaintiff and her family have routinely received medical care from providers in Defendants' network, leading to her Private Information being exposed as a result of Defendants' inadequate security. On January 3, 2020, Plaintiff received a notification letter from Defendants stating that Defendants had determined that information contained in the stolen emails "may have included your name, health insurance information, and clinical information related to treatment you received at [Health Quest] or one of our affiliates." The Notice Letter advised Plaintiff to "regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately." In response to this Notice, Plaintiff purchased credit monitoring services.

13. Plaintiff would not have obtained medical services from providers in Defendants' network had Defendants told her that they failed to maintain adequate computer systems and data security practices to safeguard her Private Information from theft.

14. Plaintiff and the other Class members have suffered actual injury and at risk of further imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being stolen in the Security Breach. To mitigate against the increased likelihood of identity theft and fraud, Plaintiff has purchased credit monitoring services. Plaintiff has begun the process of reviewing her and her family's records in order to determine whether the breach of their Private Information has led to any

fraudulent actions. Plaintiff will also need to be particularly vigilant in the years to come in order to try to identify and counter any fraudulent activity that may occur.

15. Plaintiff has a continuing interest in ensuring that her Private Information is protected and safeguarded from future breaches.

16. The injuries suffered by Plaintiff and Class members as a direct result of the Security Breach include one or more of the following:

a. unauthorized use of their Private Information;

b. theft of their Private Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Private Information;

e. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Security Breach, including reviewing records for fraudulent charges and healthcare services billed for but not received, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach;

f. damages to and diminution in value of their Private Information entrusted to Defendants for the sole purpose of purchasing products and services from Defendants; and

g. and the loss of Plaintiff's and Class members' privacy.

Defendants

17. Defendant Nuvance Health is a not-for-profit health system providing patient care in New York State's Mid-Hudson Valley region and western Connecticut. In or around April 3, 2019, Nuvance Health was created by the merging of Health Quest and Western Connecticut Health Network. Nuvance Health employs approximately 2,600 doctors and 12,000 professional staff, and serves an area with approximately 1.5 million residents from New York and Connecticut. Nuvance Health's headquarters are located at 1351 Route 55, LaGrangeville, New York 12540.

18. Defendant Health Quest Systems, Inc. is a New York not-for-profit corporation which operates a group of nonprofit hospitals and healthcare providers in the Mid-Hudson Valley in New York and in northwestern Connecticut. Health Quest Systems, Inc's headquarters are located at 1351 Route 55, LaGrangeville, NY 12540.

IV. FACTUAL BACKGROUND

19. Defendants provide healthcare services to thousands of patients per year in New York and Connecticut. As part of its business, Defendants store a vast amount of their patients' Private Information. In doing so, Defendants were entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

20. In July of 2018, Defendants first learned of a "phishing" incident whereby an unauthorized party may have gained access to the emails and attachments of several of Defendants' employee email accounts that may have contained patients' Private Information including names, dates of birth, Social Security numbers, driver's license numbers, financial account information, PINs and security codes, payment card information, provider names, dates of treatment, treatment and diagnosis information and health insurance claims information.

21. Upon learning of the Security Breach in July 2018, Defendants hired an outside cybersecurity firm to assist with an investigation of the Security Breach. The initial investigation did not conclude until April 2, 2019, almost a year after the Security Breach was uncovered by Defendants. As a result of the Security Breach, Defendants initially estimated that the Private Information of 28,910 patients was potentially compromised stemming from services received between January 2018 and June 2018. Moreover, despite the investigation concluding in early April 2019, Defendants inexplicably did not begin to notify any potentially affected patients or the public of the breach until almost two months later, in late May or early June 2019.

22. On or about January 16, 2020, Defendants announced that, following a second investigation into the July 2018 Security Breach, they had discovered that more Private Information has been compromised during the breach than previously thought, with additional patients having been affected. Defendants posted the following notice on their website:

> Health Quest is committed to protecting the confidentiality and security of our patients' and employees' information. Regrettably, this notice concerns an incident involving some of that information.
>
> On October 25, 2019, through our investigation of a phishing incident, we determined some patient information may have been contained in an email account, accessed by an unauthorized party. We first learned of a potential incident in July 2018, when numerous Health Quest employees were deceived by a phishing scheme. This resulted in certain Health Quest employees being tricked into inadvertently disclosing their email account credentials to an unauthorized party. The employee email accounts in question were secured and a leading cybersecurity firm was engaged to assist us in our investigation. As part of the investigation, we performed a comprehensive review of the voluminous contents of the email accounts in question to determine if they contained any sensitive information. HQ mailed some notification letters in May, 2019. Upon further investigation, HQ determined additional notices were required.
>
> We determined emails and attachments in some employees' email accounts contained information pertaining to current and former patients and employees. The information involved varied by individual, but may include names in combination with, dates of birth, Social Security numbers, Medicare Health Insurance Claim Numbers (HICNs), driver's license numbers, provider name(s), dates of treatment, treatment and diagnosis information, health insurance plan member and group numbers, health insurance claims

> information, financial account information with PIN/security code, and payment card information.
>
> We have no indication any patient information was viewed by the unauthorized person or has been misused. However, out of an abundance of caution, we began mailing letters to affected patients on January 10, 2020, and have established a dedicated call center to answer questions patients may have. If you have any questions regarding this incident, please call 1-844-967-1236, Monday through Friday, between 9 a.m. and 6:30 p.m. EST.
>
> We deeply regret any inconvenience or concern this incident may cause you. We continually evaluate and modify our practices to enhance the security and privacy of our patients' and employees' information. To help prevent something like this from happening in the future, we have implemented multi-factor authentication for email and additional procedures to further expand and strengthen security processes. We are also providing additional training to HQ employees regarding phishing emails and other cybersecurity issues.

Defendants did not provide any reason for why a second investigation of the same breach was necessary or detail the number of additional patients who may have been affected by the Security Breach.

23. In a notice mailed to Plaintiff by Defendants on January 3, 2020, Defendants stated in pertinent part:

> Dear Leah Wallace,
>
> At Health Quest Systems, Inc. ("HQ"), we are committed to protecting the confidentiality and security of our patients' information. Therefore, we regret to inform you about our ongoing investigation of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.
>
> On October 25, 2019, through our investigation of a phishing email incident, HQ determined that some of your information may have been contained in employee email accounts accessed by an unauthorized party. HQ first learned of a potential incident in July 2018, when numerous HQ employees were deceived by a phishing scheme, which resulted in certain HQ employees being tricked into inadvertently disclosing their email account credentials to an unauthorized party. Upon learning of the incident, the employee email accounts in question were secured and a leading cyber security firm was engaged to assist us to investigate this matter.
>
> As part of the investigation, HQ performed a comprehensive review of the voluminous contents of the email accounts in question to determine if they contained any sensitive

> information. Through this time-consuming review, which was completed on November 8, 2019, HQ determined that the information contained in the accounts may have included your name, health insurance information, and clinical information related to treatment you received at HQ or one of our affiliates.
>
> Although, to date, we have no evidence that any of your information has been misused or was in fact viewed or accessed, out of an abundance of caution, we wanted to let you know this happened and assure you we take it very seriously. We recommend that you regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately.
>
> We regret any inconvenience or concern this may cause you. We are taking steps to help prevent a similar incident from occurring in the future, including the implementation of multi-factor authentication for email, as well as additional procedures to further strengthen and expand our security processes. We are also providing additional training to our employees regarding phishing emails and other cybersecurity issues.

Defendants Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patients' Private Information

24. Defendants failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information for months. Defendants also failed to properly monitor its systems. Had it properly monitored its systems, it would have discovered the intrusion much sooner than seven months after the breach began.

25. Defendants failed to ensure that proper data security safeguards were being implemented throughout the breach period.

26. Defendants had obligations created by HIPAA, industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

27. Plaintiff and Class members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants and any of its affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

28. Prior to and during the Security Breach, Defendants promised patients that their Private Information would be kept confidential. For example, Health Quest Medical Practice, P.C.'s Notice of Privacy Practices, with an effective date of July 3, 2014, states in its "**PLEDGE REGARDING MEDICAL INFORMATION**" that "[w]e understand that medical information about you and your health is personal. We are committed to protecting medical information about you." [1] The Notice further stated that "[w]e will notify you in writing if we discover a breach of your unsecured health information, unless we determine, based on a risk assessment, that notification is not required by applicable law. You will be notified without unreasonable delay and no later than 60 days after discovery of the breach. Such notification will include information about what happened and what has been done or can be done to mitigate any harm to you as a result of such breach." *Id.*

29. Defendants' failure to provide adequate security measures to safeguard patients' Private Information is especially egregious because Defendants operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

30. In fact, Defendants have been on notice for years that the medical industry is a prime target for scammers because of the amount of confidential patient information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches including Quest Diagnostics and LabCorp.

[1] https://www.healthquest.org/Uploads/Public/Documents/Compliance/English/NOPP-Health-Quest-Medical-Practice.pdf.

31. According to a Privacy Rights Clearinghouse study entitled "Just in Time Research: data breaches in Higher Education,"[2] the medical industry accounted for 27% of all reported data breaches in the last decade, more than any other industry.

Defendants' Data Security Failures and HIPAA Violations

32. Defendants' data security lapses demonstrate that failed to honor their duties and promised by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting patients' Private Information;

c. Properly monitoring their own data security systems for existing intrusions;

d. Ensuring that they employed reasonable data security procedures;

e. Ensuring the confidentiality and integrity of electronic protected health information ("PHI") they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Implementing technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

[2] *Available at* https://library.educause.edu/~/media/files/library/2014/5/ecp1402-pdf.pdf.

h. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Protecting against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

l. Training all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

Damages to Plaintiff and the Class

33. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Security Breach.

34. Plaintiff and the Class face a substantial risk of out of pocket fraud losses such as, *e.g.*, loans opened in their names, medical services billed in their name, tax return fraud, utility bills opened in their name, credit card fraud, and similar identity theft.

35. Class members may also incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly

related to the Security Breach. Plaintiff here purchased credit monitoring out of pocket in response to being notified of the Security Breach.

36. Plaintiff and Class members suffered a "loss of value" of their Private Information when it was acquired by cyber thieves in the Security Breach. Numerous courts have recognized the propriety of "loss of value" damages in data breach cases.

37. Class members who paid Defendants for their services were also damaged via "benefit of the bargain" damages. Such members of the Class overpaid for a service that was intended to be accompanied by adequate data security, but was not. Part of the price Class members paid to Defendants was intended to be used by Defendants to fund adequate data security. Defendants did not properly comply with their data security obligations. Thus, the Class members did not get what they paid for.

38. Members if the Class have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

39. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[3]

40. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[4]

---

[3] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf.

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes

41. The theft of Social Security Numbers, which were purloined as part of the Security Breach, is particularly detrimental to victims. The U.S. Social Security Administration (SSA) warns that "[i]dentity theft is one of the fastest growing crimes in America."[5] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought." *Id.* In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems." *Id.*

42. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit." *Id.*

43. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the medical context, Private Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name. As a result, Plaintiff and members of the Class now face a real and continuing

"identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id.*

[5] Identity Theft And Your Social Security Number, Social Security Administration (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit and tax filings for an indefinite duration.

44. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendants knew or should have known this and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

The Monetary Value of Privacy Protections and Private Information

45. The fact that Plaintiff's and Class members' Private Information was stolen—and might presently be offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

46. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[6]

47. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[7]

---

[6] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001) available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[7] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

48. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[8]

49. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[9] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

50. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[10]

51. The value of Plaintiff's and Class members' Private Information on the black market is substantial, ranging, for example, from $1.50 to $90 per payment card number.[11]

52. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Private Information they maintain is highly sensitive and could be used for wrongful

---

[8] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.
[9] *Web's Hot New Commodity: Privacy*, *supra* note 7.
[10] *See* DOJ, *Victims of Identity Theft, 2014*, *supra* note 3, at 6.
[11] Leapfrog, *The Cyber Black Market: What's Your Bank Login Worth* (Mar. 1, 2011), available at https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/.

purposes by third parties, such as identity theft and fraud. Defendants should have particularly been aware of these risks given the significant number of data breaches affecting the medical industry.

53. Had Defendants remedied the deficiencies in their security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendants would have prevented intrusion into their systems and, ultimately, the theft of their patients' Private Information.

54. Given these facts, any company that transacts business with patients and then compromises the privacy of patients' Private Information has thus deprived patients of the full monetary value of their transaction with the company.

55. Acknowledging the damage to Plaintiff and Class members, Defendants instructed patients like Plaintiff to "regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately." Plaintiff and the other Class members now face a greater risk of identity theft.

V. CLASS ACTION ALLEGATIONS

56. Plaintiff bring all counts, as set forth below, on behalf of herself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Nationwide Class defined as:

> All persons who submitted their Private Information to Defendants or Defendants' affiliates and whose Private Information was compromised as a result of the data breach discovered in or about July 2018 (the "Nationwide Class").

57. In addition to and/or in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of the following subclass:

> All residents of New York who submitted their Private Information to Defendants or Defendants' affiliates and whose Private Information was compromised as a result of the data breach discovered in or about July 2018 (the "New York Subclass," collectively with the Nationwide Class, the "Class").

58. Excluded from both the Nationwide Class and the New York Subclass are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

59. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

60. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class and New York Subclass both number in the tens of thousands.

61. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants' data security systems prior to and during the Security Breach complied with applicable data security laws and regulations including, *e.g.,* HIPAA;

b. Whether Defendants' data security systems prior to and during the Security Breach were consistent with industry standards;

c. Whether Defendants properly implemented their purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendants took reasonable measures to determine the extent of the Security Breach after they first learned of same;

e. Whether Defendants disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendants' conduct constitutes breach of an implied contract;

g. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

h. Whether Defendants were negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

i. Whether Defendants' were unjustly enriched by their actions; and

j. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

62. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

63. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiff.

64. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class and the New York Subclass because her interests do not conflict with the interests of the Classes she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

65. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

66. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and

the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

67. Plaintiff repeats and re-allege Paragraphs 1 through 66 as if fully set forth herein.

68. Upon Defendants' accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

69. Defendants owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

70. Defendants owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

71. Defendants also breached their duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

72. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches within the medical industry.

73. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' Private Information.

74. Defendants breached their duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

75. Because Defendants knew that a breach of their systems would damage thousands of their customers, including Plaintiff and Class members, Defendants had a duty to adequately protect their data systems and the Private Information contained thereon.

76. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants

were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

77. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

78. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

79. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

80. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendants' misconduct included failing to: (1) secure Plaintiff's and the Class's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

81. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide

timely notice of the Security Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendants' networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

e. Failing to timely notify Class members about the Security Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

82. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendants' possession or control.

83. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

84. Neither Plaintiff nor the other Class members contributed to the Security Breach and subsequent misuse of their Private Information as described in this Complaint.

85. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

86. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

87. Plaintiff repeats and re-alleges the allegations contained in Paragraphs 1 through 66 as if fully set forth herein.

88. Defendants solicited and invited Class members to provide their Private Information as part of Defendants' regular business practices. When Plaintiff and Class members made and paid for purchases of Defendants' services and products, they provided their Private Information to Defendants.

89. In so doing, Plaintiff and Class members entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

90. Class members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

91. Plaintiff and Class members would not have provided and entrusted their Private Information with Defendants in the absence of the implied contract between them and Defendants.

92. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

93. Defendants breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the data breach within a reasonable time.

94. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants, Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

95. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members.

COUNT III
Unjust Enrichment/Quasi-Contract
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

96. Plaintiff repeats and re-allege the allegations contained in paragraphs 1 through 66 as though fully set forth herein.

97. Plaintiff and Class members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and provided Defendants with their Private Information. In exchange, Plaintiff and Class members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their Private Information with adequate data security.

98. Defendants knew that Plaintiff and Class members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendants profited from Plaintiff's purchases and used Plaintiff's and Class members' Private Information for business purposes.

99. Defendants failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class members' Private Information provided.

100. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

101. If Plaintiff and Class members knew that Defendants would not secure their Private Information using adequate security, they would not have made purchases at Defendants' stores.

102. Plaintiff and Class members have no adequate remedy at law.

103. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

104. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

105. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 through 66 as though fully set forth herein.

106. At all times during Plaintiff's and Class members' interactions with Defendants, Defendants were fully aware of the confidential, novel, and sensitive nature of Plaintiff's and Class members' Private Information that Plaintiff and Class members provided to Defendants.

107. As alleged herein and above, Defendants' relationship with Plaintiff and Class members was governed by expectations that Plaintiff's and Class members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

108. Plaintiff and Class members provided their respective Private Information to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the Private Information to be disseminated to any unauthorized parties.

109. Plaintiff and Class members also provided their respective Private Information to Defendants with the explicit and implicit understanding that Defendants would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of information security practices.

110. Defendants voluntarily received in confidence Plaintiff's and Class members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

111. Due to Defendants' failure to prevent, detect, and/or avoid the Security Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class members' Private Information, Plaintiff's and Class members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

112. But for Defendants' disclosure of Plaintiff's and Class members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Security Breach was the direct and legal cause of the theft of Plaintiff's and Class members' Private Information, as well as the resulting damages.

113. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class members' Private Information. Defendants knew or should have known their security systems were insufficient to protect the Private Information that is coveted by thieves worldwide. Defendants also failed to observe industry standard information security practices.

114. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

COUNT V
Violations of New York Consumer Law for Deceptive Acts and Practices
N.Y. Gen. Bus. Law § 349
(On Behalf of all Plaintiff and the Nationwide Class or, alternatively, by Plaintiff on behalf of the New York Subclass)

115. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1 through 66 as though fully set forth herein.

116. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

117. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

118. Defendants stored Plaintiff's and the Class members' Private Information in Defendants' electronic databases. Defendants knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiff's and the Class members' Private Information secure and prevented the loss or misuse of Plaintiff's and the Class members' Private Information. Defendants did not disclose to Plaintiff and the Class members that their data systems were not secure.

119. Plaintiff and the Class never would have provided their sensitive and personal Private Information if they had been told or knew that Defendants failed to maintain sufficient security to keep such Private Information from being hacked and taken by others, and that Defendants failed to maintain the information in encrypted form.

120. Defendants violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendants' many systems and services, specifically the security thereof, and their ability to safely store Plaintiff's and the Class members' Private Information.

121. Defendants also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and the Class members of the Security Breach. If Defendants had complied with these legal requirements, Plaintiff and the other Class members would not have suffered the damages related to the Security Breach.

122. Defendants' practices, acts, policies and course of conduct violate NYGBL § 349 in that, *inter alia*:

a. Defendants actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the Class at the time they provided such Private Information that Defendants did not have sufficient security or mechanisms to protect Private Information;

b. Defendants failed to give timely warnings and notices regarding the defects and problems with their system(s) of security systems that they maintained to protect Plaintiff's and the Class' Private Information.

123. Plaintiff and the Class were entitled to assume, and did assume, Defendants would take appropriate measures to keep their Private Information safe. Defendants did not disclose at any time that Plaintiff's and the Class' Private Information was vulnerable to hackers because Defendants' data security measures were inadequate, and Defendants were the only one in possession of that material information, which they had a duty to disclose.

124. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Defendants have, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system they maintained and failed to reveal the Security Breach timely and adequately.

125. Members of the public were deceived by and relied upon Defendants' affirmative misrepresentations and failures to disclose.

126. Such acts by Defendants are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendants. Said deceptive acts and practices are material. The requests for and use of such

Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, NYGBL § 349.

127. Defendants' wrongful conduct caused Plaintiff and the Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the Private Information materials by third parties and placing the Plaintiff and the Class at serious risk for monetary damages.

128. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

129. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class seek statutory damages for each injury and violation which has occurred.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendants, as follows:

A. Declaring that this action is a proper class action, certifying the Nationwide Class and New York Subclass as requested herein, designating Plaintiff as Nationwide Class and New York Subclass Representative, and appointing Class Counsel as requested in Plaintiff's expected motion for class certification;

B. Ordering Defendants to pay actual damages to Plaintiff and the other members of the Class;

C. Ordering Defendants to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

D. Ordering injunctive relief requiring Defendants to, *e.g.*: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members;

E. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff and their counsel;

F. Ordering Defendants to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

G. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

H. Ordering such other and further relief as may be just and proper.

Date: January 21, 2020

Respectfully submitted,

THE SULTZER LAW GROUP P.C.

By: */s/ Jason P. Sultzer*

Jason P. Sultzer
sultzerj@thesultzerlawgroup.com
85 Civic Center Plaza, Suite 200
Poughkeepsie, New York 12601
Tel: (845) 483-7100
Fax: (888) 749-7747

Counsel for Plaintiff and the Class